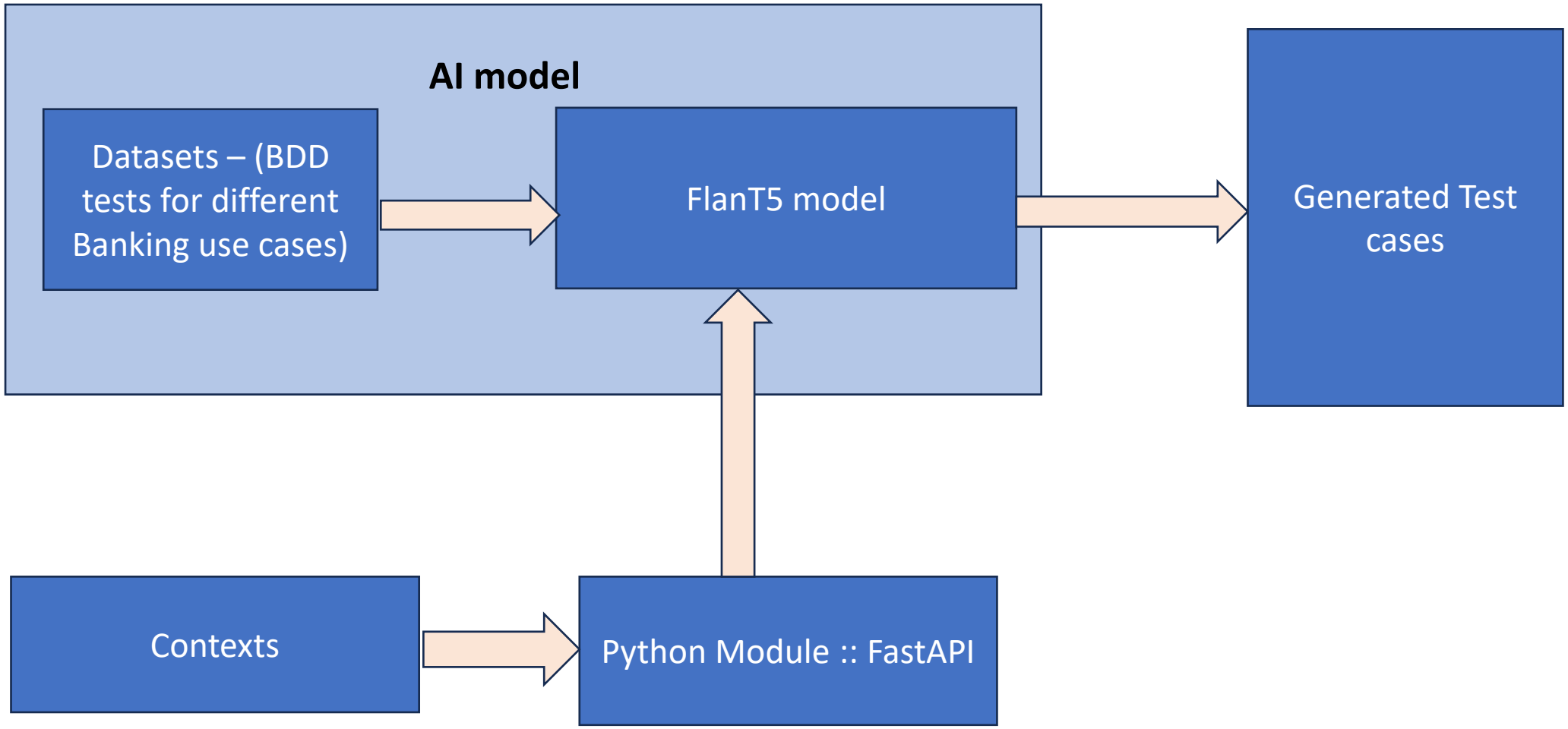
Context aware testing System for financial ecosystem

Objective

- Design and implement a context-aware testing system that can dynamically generate test case for financial transactions, customer interactions, Fraud detection, compliance and risk assessments.

High level Design



High level Design (Continued)

AI Model FLAN-T5 - is an open-source, sequence-to-sequence, large language model, provided by the HuggingFace transformers library. The model was published by Google researchers in late 2022, and has been fine-tuned on multiple tasks. This is a transformer model for NLP, which excels in few shot learning. Since the volume of data sets were limited, we found Flan T5 as a better option. We have fine tuned this model specifically for generating BDD testcases. The inference from the model is obtained via a WEB API call.

FASTApi - is a high-performing web framework for building APIs with Python. Here it is used to create an api end point '/predict' which takes the contexts as input and outputs the testcases generated by the model

Contexts - are read from a text file.

How to run

- Expose the python module as a web server using the command uvicorn main:app
- Once the server starts execute python test_api.py

  - This reads the contexts from the ./context.txt file, and makes a post request http://localhost:8000/predict which provides the test cases as a response.

Screen shots

contexts.txt

File Edit View

```
money laundering
fake login
fraud risk
```

Command Prompt | Command Prompt

```
C:\learnings\hackathon\testcasegeneration>python test_api.py
Contexts:  ['money laundering', 'fake login', 'fraud risk']
********************
Feature: Rapid Fund Transfers Across Multiple Accounts
Scenario: Detect money laundering through layering

Given a customer receives $50,000 from an unknown source
And transfers the full amount to five different accounts within an hour
When the system analyzes transaction patterns
Then the system should flag the transactions as suspicious
And notify the compliance team for review


********************


Feature: Email New Account
Scenario: Detect bulk email accounts from falsified email credentials

Given a customer logs in from $9,500 to $9,500 within 24 hours
When the system verifies the account review
When the system makes further improvements the system can correct
Then the system should flag the account for a login attempt
When the system processes the login attempt the system should the login be rejected


********************
```

Screen shots (Continued)

```
**********************


Feature: New Account Monitoring
Scenario: Identify fraudulent logins

Given a customer logs in from a fraudulent login
When the system evaluates login patterns
Then the system should flag the login as suspicious
And notify the customer with a rare


**********************
```

Limitations

The model accuracy is only satisfactory, as the volume of data used to train the model is very less (around 100)

Future enhancements

- Train the model with huge volume of data, to improve model predictions and accuracy.
- The model should learn consistently with new contexts.
- The model should dynamically identify the change in contexts and generate test cases.